

# POLYNOMIALS WHOSE REDUCIBILITY IS RELATED TO THE GOLDBACH CONJECTURE

PETER BORWEIN, KWOK-KWONG STEPHEN CHOI, GREG MARTIN,  
AND CHARLES L. SAMUELS

**ABSTRACT.** We introduce a collection of polynomials  $F_N$ , associated to each positive integer  $N$ , whose divisibility properties yield a reformulation of the Goldbach conjecture. While this reformulation certainly does not lead to a resolution of the conjecture, it does suggest two natural generalizations for which we provide some numerical evidence. As these polynomials  $F_N$  are independently interesting, we further explore their basic properties, giving, among other things, asymptotic estimates on the growth of their coefficients.

## 1. INTRODUCTION

Let  $\mathcal{P}$  denote the set of odd primes. One of the oldest unsolved problems in mathematics concerns the set  $\mathcal{P} + \mathcal{P} = \{p + q : p, q \in \mathcal{P}\}$ .

**Conjecture 1.1** (Goldbach Conjecture). If  $N > 4$  is an even integer, then  $N \in \mathcal{P} + \mathcal{P}$ .

If  $N$  is any positive integer, we say that the *Goldbach conjecture holds for  $N$*  if  $N \in \mathcal{P} + \mathcal{P}$ . Otherwise, we say the *Goldbach conjecture fails for  $N$* . Of course, we make no attempt here to prove the Goldbach conjecture, however we wish to study a related collection of polynomials. In order to construct these polynomials, we let  $\chi_{\mathcal{P}} : \mathbb{N} \rightarrow \{0, 1\}$  denote the indicator function of  $\mathcal{P}$ . That is,

$$\chi_{\mathcal{P}}(n) = \begin{cases} 1 & \text{if } n \text{ is an odd prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, for each positive integer  $N$ , we define

$$R(N) = \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(N-n)$$

so that  $R(N)$  counts the number of ways to write  $N$  as a sum of two odd primes. We note that  $R(N) = 0$  if and only if  $N \notin \mathcal{P} + \mathcal{P}$ . To each positive integer  $N$ , we associate a polynomial  $F_N \in \mathbb{Z}[x]$  given by

$$F_N(z) = \sum_{k=0}^{N-1} \left( \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) z^{kn} \right)^2.$$

Our first result shows that the  $F_N(z)$  are closely related to the Goldbach problem. In this article, we will always use  $\Phi_N$  to denote the  $N$ th cyclotomic polynomial.

---

*Date:* August 22, 2014.

Research of all authors is supported in part by NSERC of Canada.

**Theorem 1.2.** *Suppose that  $N$  is a positive integer. Then  $\Phi_N$  divides  $F_N$  if and only if the Goldbach conjecture fails for  $N$ .*

In other words, Theorem 1.2 reformulates the Goldbach conjecture in terms of the divisibility properties of  $F_N$ . Since no odd integer can be written as a sum of odd primes, we observe immediately that  $\Phi_N$  divides  $F_N$  for all odd  $N$ . Naively, it is reasonable to conjecture that  $F_N$  is irreducible for all even integers  $N > 4$ . Unfortunately,  $F_N$  always has at least one non-trivial irreducible factor.

**Theorem 1.3.** *If  $N$  is a positive integer then  $\Phi_{2N}$  divides  $F_N$ .*

Early numerical evidence seems to suggest that  $F_N/\Phi_{2N}$  is, in fact, irreducible for all even integers  $N > 4$ . If this is the case, then the Goldbach conjecture would follow. Similarly, it appears that, for odd integers  $N > 5$ , we have that  $F_N/(\Phi_N\Phi_{2N})$  is irreducible. Although this is not relevant to the Goldbach conjecture, we find it independently interesting.

**Conjecture 1.4.** *If  $N > 5$  is an integer then the following conditions hold.*

- (i) *If  $N$  is even, then  $F_N/\Phi_{2N}$  is irreducible.*
- (ii) *If  $N$  is odd, then  $F_N/\Phi_N\Phi_{2N}$  is irreducible.*

As we have noted, Conjecture 1.4 (i) would imply the Goldbach conjecture. However, the converse is possibly false. Indeed,  $F_N/\Phi_{2N}$  could be reducible but still not divisible by  $\Phi_N$ . As such, we should view Conjecture 1.4 as being significantly harder than the Goldbach conjecture, and therefore, not likely within reach using current techniques. Nonetheless, we find it interesting to see the Goldbach conjecture in this context.

As evidence in favor of Conjecture 1.4, we have found that it holds for all  $N \leq 50$ . For even  $N$ , the first few polynomials  $F_N/\Phi_N$  are given in the following list.

$$\begin{aligned}
F_6/\Phi_{12} &= z^{46} + z^{44} - z^{40} - z^{38} + 3z^{36} + 4z^{34} + z^{32} - 3z^{30} - 2z^{28} + 3z^{26} \\
&\quad + 5z^{24} + 2z^{22} - 2z^{18} - z^{16} + 2z^{14} + 5z^{12} + 3z^{10} - z^8 - 3z^6 + 4z^2 + 4 \\
F_8/\Phi_{16} &= z^{90} - z^{82} + 3z^{76} + z^{74} - 3z^{68} - z^{66} + 2z^{64} + 4z^{62} + 3z^{60} + z^{58} \\
&\quad - 2z^{56} - 4z^{54} + 2z^{52} - z^{50} + 5z^{48} + 4z^{46} - 2z^{44} + 4z^{42} - z^{40} \\
&\quad - 4z^{38} + 2z^{36} - 2z^{34} + 6z^{32} + 4z^{30} + z^{28} + 2z^{26} - 4z^{24} - 2z^{18} \\
&\quad + 9z^{16} + 3z^{12} + 3z^{10} - 7z^8 + z^6 + 9 \\
F_{10}/\Phi_{20} &= z^{118} + z^{116} - z^{108} - z^{106} + z^{104} + z^{102} + 2z^{100} + 3z^{98} + z^{96} - z^{94} \\
&\quad - z^{92} - z^{90} + z^{86} + z^{84} + 4z^{82} + 4z^{80} + 2z^{76} + 2z^{74} - z^{72} - z^{70} \\
&\quad - 2z^{66} + 2z^{64} + 9z^{62} + 5z^{60} + 4z^{56} - 4z^{52} + 3z^{48} + z^{44} + 7z^{42} + 8z^{40} \\
&\quad + 2z^{38} + z^{34} - 3z^{30} + z^{28} + 3z^{26} + z^{24} + 6z^{22} + 8z^{20} + 2z^{16} \\
&\quad + 4z^{14} - 3z^{12} - 4z^{10} + 3z^8 + z^6 + 9z^2 + 9.
\end{aligned}$$

Now we give the analogous list but for odd  $N$ .

$$\begin{aligned}
F_7/(\Phi_7\Phi_{14}) &= z^{48} - z^{46} + z^{38} + z^{36} - z^{34} - z^{32} + 3z^{28} - 3z^{26} + 2z^{24} \\
&\quad + z^{20} - z^{18} - 2z^{16} + 3z^{14} - z^{10} + z^8 + z^6 - 4z^2 + 4 \\
F_9/(\Phi_9\Phi_{18}) &= z^{100} - z^{94} + z^{86} + 2z^{84} + z^{82} - z^{80} - 2z^{78} - z^{76} + 3z^{72} \\
&\quad + 4z^{68} - z^{66} + z^{64} - 4z^{62} + 3z^{58} + z^{54} - 2z^{52} + 4z^{50} + 4z^{48} \\
&\quad - z^{46} - z^{44} - 5z^{42} + 3z^{40} + 6z^{36} - 2z^{34} + z^{32} + z^{30} + 4z^{28} \\
&\quad - z^{26} - 4z^{24} - 2z^{22} + 2z^{20} + 7z^{18} - z^{16} - z^{14} + 2z^{12} + 3z^{10} \\
&\quad + 2z^8 - 8z^6 + 9 \\
F_{11}/(\Phi_{11}\Phi_{22}) &= z^{120} - z^{118} + z^{106} - z^{104} + 2z^{100} - z^{98} - z^{96} + z^{92} - z^{90} \\
&\quad + 2z^{88} - 2z^{86} + z^{84} - z^{82} + 3z^{80} - 3z^{74} + 4z^{70} - 4z^{68} + 2z^{66} \\
&\quad + z^{64} - 2z^{62} + 4z^{60} - 2z^{58} + z^{52} - 4z^{46} + 4z^{44} - z^{42} + 4z^{40} \\
&\quad - 2z^{38} + z^{36} - 2z^{34} - z^{32} + 4z^{30} + 2z^{28} - 5z^{26} - 4z^{24} + 6z^{22} \\
&\quad + 2z^{20} - z^{18} + z^{16} - 2z^{14} + z^{10} + z^8 + z^6 - 9z^2 + 9.
\end{aligned}$$

Indeed, we have found that the right hand sides on the above lists are all irreducible over  $\mathbb{Z}$ .

Because of their relevance to the Goldbach conjecture, it may also be interesting to study the number of roots of  $F_N$  that lie on the unit circle. In view of Theorem 1.3, it is clear that  $F_N$  has at least  $\varphi(2N)$  such roots. For even integers  $N > 4$ , if  $F_N$  has no other roots on the unit circle, then the Goldbach conjecture would follow from Theorem 1.2. Our numerical evidence suggests this to be the case. Furthermore, when  $N$  is odd, we know that  $F_N$  must, in fact, have at least  $\varphi(2N) + \varphi(N)$  roots on the unit circle. Again, our evidence suggests that there are no others. Also, the identity

$$\varphi(2N) = \begin{cases} 2\varphi(N) & \text{if } N \text{ is even} \\ \varphi(N) & \text{if } N \text{ is odd.} \end{cases}$$

holds for all positive integers  $N$ . So we pose the following strengthening of the Goldbach conjecture.

**Conjecture 1.5.** If  $N > 5$  is an integer then  $F_N$  has precisely  $2\varphi(N)$  roots on the unit circle.

Similar to our note above, the converse of Conjecture 1.5 is not necessarily true.  $F_N$  could have many roots on the unit circle while still not being divisible by  $\Phi_N$ . Once again, this conjecture should be regarded as more difficult than the Goldbach conjecture.

We also observe that Conjecture 1.5 is a consequence of Conjecture 1.4. Indeed, for the case of even  $N$ , if  $F/\Phi_{2N}$  is irreducible and has a root on the unit circle, then it must be reciprocal, which it certainly is not. Similar remarks apply to  $F/(\Phi_N\Phi_{2N})$  when  $N$  is odd.

We have computed the number of roots of  $F_N$  on the unit circle for  $N \leq 50$  and have found that Conjecture 1.5 holds for those  $F_N$ . This complete list is given in Table 1 including the number of roots inside, on and outside the unit circle for each  $F_N$ .

TABLE 1. Location of roots of  $F_N$ 

$N$	$2\varphi(N)$	$[ z  < 1]$	$ z  = 1$	$ z  > 1]$
6	4		[16	4 30]
7	12		[4	12 44]
8	8		[24	8 66]
9	12		[8	12 92]
10	8		[16	8 102]
11	20		[16	20 104]
12	8		[48	8 186]
13	24		[40	24 200]
14	12		[40	12 286]
15	16		[40	16 308]
16	16		[36	16 338]
17	32		[36	32 348]
18	12		[56	12 510]
19	36		[40	36 536]
20	16		[80	16 626]
21	24		[60	24 676]
22	20		[64	20 714]
23	44		[56	44 736]
24	16		[92	16 950]
25	40		[84	40 980]
26	24		[100	24 1026]
27	36		[108	36 1052]
28	24		[92	24 1126]
29	56		[100	56 1132]
30	16		[132	16 1534]
31	60		[128	60 1552]
32	32		[144	32 1746]
33	40		[136	40 1808]
34	32		[144	32 1870]
35	48		[160	48 1900]
36	24		[168	24 1978]
37	72		[136	72 2024]
38	36		[180	36 2522]
39	48		[172	48 2592]
40	32		[184	32 2670]
41	80		[176	80 2704]
42	24		[200	24 3138]
43	84		[184	84 3176]
44	40		[244	40 3414]
45	48		[252	48 3484]
46	44		[228	44 3598]
47	92		[244	92 3620]
48	32		[288	32 4098]
49	84		[260	84 4168]
50	40		[264	40 4302]

It is worth noting that, in our construction of  $F_N$ , the set of odd primes may be replaced with any subset of  $\mathbb{N}$ . In this way, one may attempt to prove theorems analogous to those stated above. One such example, which is of particular interest in number theory, arises in the following way.

The Liouville function  $\lambda : \mathbb{N} \rightarrow \{-1, 1\}$  is the completely multiplicative function such that  $\lambda(p) = -1$  at every prime  $p$ . Now define the set

$$\mathcal{L} = \{n \in \mathbb{N} : \lambda(n) = -1\}.$$

It is a direction of our future research to examine the analogs of  $F_N$  that are obtained by using the above construction with  $\mathcal{L}$  in place of  $\mathcal{P}$ . Perhaps this strategy can yield a proof that every positive even integer  $N > 2$  satisfies  $N \in \mathcal{L} + \mathcal{L}$ . On the surface, such a result appears to be easier than the Goldbach conjecture, and therefore, is possibly within reach.

One can also consider weighted forms of  $F_N$ . Similar to the study of the prime number theorem, instead of using the above indicator function of  $\mathcal{P}$ , we use the weighted form

$$\tilde{\chi}_{\mathcal{P}}(n) = \begin{cases} \log n & \text{if } n \in \mathcal{P}, \\ 0 & \text{otherwise} \end{cases}$$

and define the corresponding polynomials  $\tilde{F}_N$  by

$$\tilde{F}_N(z) = \sum_{k=0}^{N-1} \left( \sum_{n=1}^{N-1} \tilde{\chi}_{\mathcal{P}}(n) z^{kn} \right)^2.$$

It is clear that the  $\tilde{F}_N(z)$  do not have integer coefficients, so we might expect different types of results regarding these polynomials. Nonetheless, we believe they yield another interesting route for future research.

In the following two sections, we examine a series of basic properties of the polynomials  $F_N$ . Specifically in section 3, we produce estimates on the size of the coefficients of  $F_N$ , as well as asymptotic formulae for certain sums of their coefficients. The remaining sections are devoted to the proofs of our results.

## 2. PROPERTIES OF THE POLYNOMIALS $F_N$

Now that we understand the relevance of the polynomials  $F_N$  to the Goldbach conjecture, we consider some of their additional properties. We begin with the following result regarding their symmetry.

**Theorem 2.1.** *If  $N$  is a positive integer then  $F_N(z) = F_N(-z)$ .*

Theorem 2.1 certainly implies that if  $\Phi_N(z)$  divides  $F_N(z)$  then so does  $\Phi_N(-z)$ . Furthermore, we know that if  $M$  is an odd integer then  $\Phi_{2M}(z) = \Phi_M(-z)$ . Combining these observations with Theorem 1.2, we obtain the following corollary.

**Corollary 2.2.** *If  $M$  is an odd integer and  $N = 2M$  then the following conditions are equivalent.*

- (i)  $\Phi_N$  divides  $F_N$ .
- (ii)  $\Phi_M$  divides  $F_N$ .
- (iii) The Goldbach conjecture fails for  $N$ .

Suppose now that, for any positive integer  $M$ ,  $\zeta_M$  is a primitive  $M$ th root of unity. We may view Corollary 2.2 as examining the value of  $F_N(\zeta_M)$  when  $M$  is a certain divisor of  $N$ . Next, we consider the values of  $F_N(\zeta_M)$  when  $M$  is an arbitrary divisor of  $N$ . We write  $[x]$  to denote the largest integer less than or equal to  $x$ .

**Theorem 2.3.** *If  $N > 4$  is an integer and  $M \mid N$  then the following conditions hold.*

(i) *If  $M$  is odd then*

$$F_N(\zeta_M) \geq N \sum_{n=1}^{[N/2M]} R(2nM).$$

(ii) *If  $M$  is even then*

$$F_N(\zeta_M) \geq N \sum_{n=1}^{N/M} R(nM).$$

Applying Theorems 2.3 and 1.2 immediately yield the following simpler lower bound on  $F_N(\zeta_M)$ .

**Corollary 2.4.** *If  $N > 4$  is an integer and  $M \mid N$ , then  $F_N(\zeta_M) \geq NR(N)$  with equality when  $M = N$ .*

The case  $M = N$  may not be the only case of equality in Corollary 2.4. In fact, if  $M$  is odd and  $N = 2M$ , then it can be shown that  $F_N(\zeta_M) = NR(N)$  as well. This result also provides a strengthening of one direction of Theorem 1.2. If  $\Phi_M$  ever divides  $F_N$ , then it follows from Corollary 2.4 that  $R(N) = 0$ . In other words, we have established the following statement.

**Corollary 2.5.** *Suppose  $N > 4$  is an integer and  $M \mid N$ . If  $\Phi_M$  divides  $F_N$  then the Goldbach conjecture fails for  $N$ .*

The converse of Corollary (2.5) is certainly false. Otherwise,  $\Phi_1$  would divide  $F_N$  for every odd  $N$ , and it certainly does not. When restricted to even integers, it is likely true, but only because the Goldbach conjecture would imply that the hypothesis is always false. In fact, in view of Theorem 1.2, such a statement is equivalent to the Goldbach conjecture.

### 3. THE COEFFICIENTS OF $F_N$

Let us now turn our attention to understanding the coefficients of  $F_N$ . For this purpose, we note that  $\deg F_N \leq 2(N-1)^2$  and write

$$F_N(z) = \sum_{m=0}^{2(N-1)^2} a_{N,m} z^m.$$

It is easy to see that the constant term in  $F_N$  is given by the formula

$$a_{N,0} = \left( \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) \right)^2 = (\pi(N-1) - 1)^2$$

where  $\pi(N-1)$  denotes the number of primes  $p \leq N-1$ . Furthermore, by multiplying out the terms in the definition of  $F_N$ , we obtain an explicit formula for all other coefficients of  $F_N$ .

**Theorem 3.1.** *Let  $N$  be a positive integer. We have that*

$$a_{N,m} = \sum_{\substack{d|m \\ m/d < N}} \sum_{n=\max\{0, d-N\}+1}^{\min\{N, d\}-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(d-n)$$

for all  $0 < m \leq 2(N-1)^2$ .

Among other things, Theorem 3.1 shows that

$$a_{N,m} \leq \sum_{d|m} R(d)$$

with equality whenever  $0 < m \leq N$ . We can rephrase the case of equality by saying that

$$(3.1) \quad a_{N,m} = \sum_{d|m} R(d)$$

whenever  $0 < m \leq N$ . It is worth noting that the right hand side of (3.1) does not depend on  $N$ , so that the non-constant coefficients of the  $F_N(z)$  stabilize as  $N$  tends to infinity. More specifically, if we write  $a(m) = a_{N,m}$  for some  $N \geq m$ , the polynomials  $F_N(z) - a_{N,0}$  converge coefficient-wise to the power series

$$F(z) = \sum_{n=1}^{\infty} a(n)z^n.$$

It is straightforward to verify that  $F(z)$  has radius of convergence 1, and the sequence  $\{F_N(z) - a_{N,0}\}$  converges uniformly to  $F(z)$  on compact subsets of the unit disk.

Let us now examine the individual terms  $a(m)$ . If  $m$  is odd, then all divisors of  $m$  are also odd, so we conclude that  $a(m) = 0$ . Hence, it is only interesting to consider the situation where  $m$  is even, in which case the coefficients seem to behave in a rather subtle way. However, we can obtain lower bounds in relation to other famous arithmetic functions. Before proceeding, we recall that  $\omega(n)$  denotes the number of distinct prime factors of  $n$  and  $d(n)$  denotes the number of divisors of  $n$ .

**Theorem 3.2.** *If  $m > 1$  is an integer then*

$$(3.2) \quad a(2m) \geq \omega(m) - \begin{cases} 1 & \text{if } m \equiv 2 \pmod{4}, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, if the Goldbach conjecture is true, then

$$(3.3) \quad a(2m) \geq d(m) - \begin{cases} 2 & \text{if } m \text{ is even,} \\ 1 & \text{otherwise.} \end{cases}$$

We note that the right hand side of (3.2) is always positive for  $m > 2$ . So taking an integer  $m > 4$ , we have that  $a(m) = 0$  if and only if  $m$  is odd. It is also worth observing that the right hand sides of (3.2) and (3.3) are sometimes equal, namely when  $m$  is prime. In general, however,  $d(m)$  is much larger than  $\omega(m)$  so that our bound under the Goldbach conjecture is stronger than the analogous unconditional bound.

It is reasonable to expect that, not only is  $R(2d)$  positive for  $d > 2$ , but it is quite large most of the time. More specifically, Hardy and Littlewood have proposed the following asymptotic formula.

**Conjecture 3.3** (Hardy and Littlewood [3]). As  $n$  tends to infinity,

$$(3.4) \quad R(2n) \sim 2C_2 \frac{n}{\log^2 n} \prod_{\substack{p|n \\ p>2}} \frac{p-1}{p-2},$$

where  $C_2$  is the twin primes constant

$$C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right).$$

Under the assumption of Conjecture 3.3, we can improve the bounds of Theorem 3.2. If  $2^k \parallel m$ , then define

$$(3.5) \quad J(m) = \left(2 - \frac{1}{2^k}\right) \prod_{\substack{p^\ell \parallel m \\ p>2}} \left(1 - \frac{2}{p^{\ell+1}}\right) \left(1 - \frac{2}{p}\right)^{-1}.$$

Here,  $p^\ell \parallel m$  means that  $p^\ell \mid m$  but  $p^{\ell+1} \nmid m$ .

**Theorem 3.4.** *If Conjecture 3.3 is true, then*

$$a(2m) \sim \frac{2C_2 J(m)m}{\log^2 m}$$

as  $m$  tends to infinity.

For a positive integer  $M$ , it is also of interest to study the summatory function

$$A(M) = \sum_{m=1}^{2M} a(m).$$

By applying Theorem 3.2 directly, we are able to verify that

$$A(M) \geq \sum_{m=1}^M \omega(m) + O(M) = M \log \log M + O(M),$$

where the last equality is obtained from [2], page 355. If we are willing to assume the Goldbach conjecture, a similar argument reveals that

$$(3.6) \quad A(M) \geq \sum_{m=1}^M d(m) + O(M) = M \log M + O(M).$$

As we have remarked following our statement of Theorem 3.2, we anticipate that  $a(2m)$  is large much of the time. However, in order to obtain an asymptotic formula for  $a(2m)$ , we needed to assume a very strong conjecture of Hardy and Littlewood. In the case of  $A(M)$ , we can obtain such a formula unconditionally.

**Theorem 3.5.** *We have that*

$$A(M) = \frac{\pi^2 M^2}{3 \log^2 M} + O\left(\frac{M^2 \log \log M}{\log^3 M}\right).$$



## 4. PROOFS OF THE RESULTS FROM SECTION 1

We begin this section with the proof to Theorem 1.2

*Proof of Theorem 1.2.* Let  $\zeta$  be a primitive  $N$ th root of unity. We have immediately that

$$\begin{aligned} F_N(\zeta) &= \sum_{k=0}^{N-1} \left( \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) \zeta^{kn} \right)^2 \\ &= \sum_{k=0}^{N-1} \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m) \chi_{\mathcal{P}}(n) \zeta^{k(m+n)} \\ &= \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m) \chi_{\mathcal{P}}(n) \sum_{k=0}^{N-1} \zeta^{k(m+n)}. \end{aligned}$$

We know that

$$\sum_{k=0}^{N-1} \zeta^{k(m+n)} = 0$$

unless  $m+n \equiv 0 \pmod{N}$ . In our case, this may occur only when  $m+n = N$ , implying that

$$F_N(\zeta) = \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(N-n) \sum_{k=0}^{N-1} \zeta^{kN} = NR(N).$$

If  $R(N) = 0$  then  $F_N(\zeta) = 0$  showing that  $\Phi_N$  must divide  $F_N$ . On the other hand, if  $\Phi_N$  divides  $F_N$ , it is obvious that  $F_N(\zeta) = 0$  so that  $R(N) = 0$ .  $\square$

We already have all of the tools necessary to prove Theorem 1.3.

*Proof of Theorem 1.3.* We must show that  $F_N(e^{\pi i/N}) = 0$ . To see this, note that

$$\begin{aligned} F_N(e^{\pi i/N}) &= \sum_{k=0}^{N-1} \left( \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) e^{\frac{\pi i kn}{N}} \right)^2 \\ &= \sum_{k=0}^{N-1} \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m) \chi_{\mathcal{P}}(n) e^{\frac{\pi i k(m+n)}{N}} \\ &= \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m) \chi_{\mathcal{P}}(n) \sum_{k=0}^{N-1} e^{\frac{\pi i k(m+n)}{N}}. \end{aligned}$$

The product  $\chi_{\mathcal{P}}(m) \chi_{\mathcal{P}}(n) = 0$  unless  $m$  and  $n$  are both odd primes. In this case, we certainly have that  $m+n$  is even so that

$$(4.1) \quad \sum_{k=0}^{N-1} e^{\frac{\pi i k(m+n)}{N}} = \sum_{k=0}^{N-1} e^{\frac{2\pi i k((m+n)/2)}{N}}.$$

Of course,  $0 < (m+n)/2 < N$  implying that the right hand side of (4.1) equals zero. In other words, we have shown that

$$\chi_{\mathcal{P}}(m) \chi_{\mathcal{P}}(n) \sum_{k=0}^{N-1} e^{\frac{\pi i k(m+n)}{N}} = 0$$

for all  $1 \leq m, n < N$ , verifying the theorem.  $\square$

## 5. PROOFS OF THE RESULTS FROM SECTION 2

*Proof of Theorem 2.1.* It follows directly from the definition that

$$(5.1) \quad F_N(-z) = \sum_{k=0}^{N-1} \left( \sum_{n=1}^{N-1} (-1)^{kn} \chi_{\mathcal{P}}(n) z^{kn} \right)^2.$$

If  $n$  is even, we certainly have that  $\chi_{\mathcal{P}}(n) = 0$ . Otherwise, we have that  $(-1)^n = -1$ , which implies that  $(-1)^{kn} \chi_{\mathcal{P}}(n) = (-1)^k \chi_{\mathcal{P}}(n)$  for all  $n$ . Using (5.1), we find that

$$F_N(-z) = \sum_{k=0}^{N-1} \left( (-1)^k \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) z^{kn} \right)^2 = \sum_{k=0}^{N-1} \left( \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) z^{kn} \right)^2 = F_N(z)$$

which completes the proof.  $\square$

In view of Theorem 2.1, we obtain our proof of Corollary 2.2 almost immediately.

*Proof of Corollary 2.2.* In view of Theorem 1.2, we immediately have that (i) if and only if (iii). To finish the proof, we will show that (i) if and only if (ii). To see this, note that since  $M$  is odd, we have that  $\Phi_N(z) = \Phi_M(-z)$ . Furthermore, Theorem 2.1 implies that  $\Phi_N(z)$  divides  $F_N(z)$  if and only if  $\Phi_N(-z)$  divides  $F_N(z)$  and the result follows.  $\square$

*Proof of Theorem 2.3.* Suppose that  $a = 1$  if  $M$  is odd and  $a = 0$  if  $M$  is even. We must show that

$$F_N(\zeta_M) \geq N \sum_{1 \leq k \leq N/(2^a M)} R(2^a k M).$$

From the definition of  $F_N$ , we have that

$$\begin{aligned} F_N(\zeta_M) &= \sum_{k=0}^{N-1} \sum_{2 < p_1, p_2 \leq N-1} \zeta_M^{k(p_1+p_2)} \\ &= \sum_{2 < p_1, p_2 \leq N-1} \sum_{i=0}^{N/M-1} \sum_{k=0}^{M-1} \zeta_M^{(iM+k)(p_1+p_2)} \\ &= \frac{N}{M} \sum_{2 < p_1, p_2 \leq N-1} \sum_{k=0}^{M-1} \zeta_M^{k(p_1+p_2)}. \end{aligned}$$

Now the inner summation over  $k$  is zero unless  $(p_1 + p_2)/M \in \mathbb{Z}$ . Hence we have

$$\begin{aligned} F_N(\zeta_M) &= N \sum_{1 \leq \ell \leq 2(N-1)/M} \sum_{\substack{2 < p_1, p_2 \leq N-1 \\ p_1+p_2=\ell M}} 1 \\ &= N \left\{ \sum_{1 \leq \ell \leq N/M} + \sum_{N/M+1 \leq \ell \leq 2(N-1)/M} \right\} \sum_{\substack{2 < p_1, p_2 \leq N-1 \\ p_1+p_2=\ell M}} 1 \\ &= N \sum_{1 \leq \ell \leq N/(2^a M)} R(2^a \ell M) + N \sum_{N/M+1 \leq \ell \leq 2(N-1)/M} \sum_{\substack{2 < p_1, p_2 \leq N-1 \\ p_1+p_2=\ell M}} 1 \\ &\geq N \sum_{1 \leq \ell \leq N/(2^a M)} R(2^a \ell M). \end{aligned}$$

and the result follows.  $\square$

*Proof of Corollary 2.4.* If  $M$  is even, we have that

$$F_N(\zeta_M) \geq N \sum_{n=1}^{N/M} R(nM) \geq NR \left( \frac{N}{M} \cdot M \right) = NR(N).$$

If  $M$  is odd and  $N$  is even, then  $N/2M \in \mathbb{N}$  so it follows that

$$F_N(\zeta_M) \geq N \sum_{n=1}^{N/2M} R(2nM) \geq NR \left( 2 \cdot \frac{N}{2M} \cdot M \right) = NR(N).$$

Finally, if  $M$  and  $N$  are both odd, then  $NR(N) = 0$  so that

$$F_N(\zeta_M) \geq N \sum_{n=1}^{\lfloor N/2M \rfloor} R(2nM) \geq 0 = NR(N).$$

$\square$

*Proof of Corollary 2.5.* If  $\Phi_M \mid F_N$  then we have that  $F_N(\zeta_M) = 0$ . It follows from Corollary 2.4 that  $R(N) = 0$ .  $\square$

## 6. PROOFS OF THE RESULTS FROM SECTION 3

*Proof of Theorem 3.1.* We first note that

$$F_N(z) = \sum_{k=0}^{N-1} \left( \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) z^{kn} \right)^2 = \sum_{k=0}^{N-1} \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m) \chi_{\mathcal{P}}(n) z^{k(m+n)}.$$

Relabeling the indices, we find that

$$\begin{aligned} F_N(z) &= \sum_{m=0}^{2(N-1)^2} \left( \sum_{\substack{d|m \\ m/d < N}} \sum_{\substack{n_1+n_2=d \\ 1 \leq n_1, n_2 < N}} \chi_{\mathcal{P}}(n_1) \chi_{\mathcal{P}}(n_2) \right) z^m \\ &= \sum_{m=0}^{2(N-1)^2} \left( \sum_{\substack{d|m \\ m/d < N}} \sum_{n=\max\{0, d-N\}+1}^{\min\{N, d\}-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(d-n) \right) z^m \end{aligned}$$

establishing the theorem.  $\square$

*Proof of Theorem 3.2.* Using Theorem 3.1, we have immediately that

$$a(2m) = \sum_{d|2m} \sum_{n=1}^{d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(d-n).$$

However, it is clear that

$$\sum_{n=1}^{d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(d-n) = 0$$

whenever  $d$  is odd, which implies that

$$\begin{aligned}
 a(2m) &= \sum_{\substack{d|2m \\ d \text{ even}}} \sum_{n=1}^{d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(d-n) \\
 (6.1) \qquad &= \sum_{d|m} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(2d-n).
 \end{aligned}$$

We now use (6.1) to prove (3.2). If  $p$  is an odd prime, we have that  $\chi_{\mathcal{P}}(p)\chi_{\mathcal{P}}(2p-p) = 1$  implying

$$(6.2) \qquad \sum_{n=1}^{2p-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(2p-n) \geq 1.$$

Now let  $\omega_{\text{odd}}(m)$  denote the number of distinct odd prime divisors of  $m$  and consider three cases according to the residue class of  $m$  modulo 4.

- (i) First assume that  $m$  is odd. In this case, we have that  $\omega_{\text{odd}}(m) = \omega(m)$  and  $m \not\equiv 2 \pmod{4}$ . The inequality (6.2) holds for every odd prime divisor  $p$  of  $m$ . Combining this observation with (6.1), we find that

$$a(2m) \geq \omega_{\text{odd}}(m) = \omega(m)$$

completing the proof in this case.

- (ii) Now assume that  $m \equiv 0 \pmod{4}$ . It is easily verified that

$$\sum_{d|4} \sum_{n=1}^7 \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(8-n) = 1,$$

and then it follows from (6.1) and (6.2) that

$$a(2m) \geq \omega_{\text{odd}}(m) + 1.$$

Since 2 divides  $m$ , we have that  $\omega_{\text{odd}}(m) = \omega(m) - 1$  establishing the result in this case.

- (iii) Finally, we consider the case that  $m \equiv 2 \pmod{4}$ . Again,  $m$  is even so that  $\omega_{\text{odd}}(m) = \omega(m) - 1$ , and we conclude from (6.1) and (6.2) that  $a(2m) \geq \omega_{\text{odd}}(m)$ . This completes the proof of (3.2).

To establish (3.3), we assume that the Goldbach Conjecture holds. Hence, we have that

$$(6.3) \qquad \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(2d-n) \geq 1$$

for all divisors  $d$  of  $m$  with  $d \notin \{1, 2\}$ . Here we consider two cases.

- (i) Suppose first that  $m$  is odd. Here, we have that (6.3) holds for all divisors  $d$  of  $m$  different than 1. This gives

$$\begin{aligned} a(2m) &= \sum_{d|m} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(2d-n) = \sum_{\substack{d|m \\ d \neq 1}} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(2d-n) \\ &\geq \sum_{\substack{d|m \\ d \neq 1}} 1 = d(m) - 1 \end{aligned}$$

completing the proof in this case.

- (ii) In the case that  $m$  is even, we have that (6.3) holds except when  $d = 1$  or  $d = 2$ . Therefore, we have that

$$\begin{aligned} a(2m) &= \sum_{d|m} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(2d-n) = \sum_{\substack{d|m \\ d \notin \{1,2\}}} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n) \chi_{\mathcal{P}}(2d-n) \\ &\geq \sum_{\substack{d|m \\ d \notin \{1,2\}}} 1 = d(m) - 2 \end{aligned}$$

which completes the proof in this case as well.  $\square$

We now move on to a proposition from which we will deduce Theorem 3.4. Define

$$f(n) = \prod_{\substack{p|n \\ p > 2}} \frac{p-1}{p-2}$$

to be the multiplicative function appearing in Conjecture 3.3, and note that if  $k \geq 0$  is the integer such that  $2^k \parallel m$ , then

$$\begin{aligned} \sum_{d|m} df(d) &= \prod_{p^\ell \parallel m} \sum_{d|p^\ell} df(d) \\ &= \prod_{p^\ell \parallel m} (1 + pf(p) + p^2 f(p^2) + \cdots + p^\ell f(p^\ell)) \\ &= \left(1 + 2 \frac{2^k - 1}{2 - 1}\right) \prod_{\substack{p^\ell \parallel m \\ p > 2}} \left(1 + \frac{p-1}{p-2} \cdot p \frac{p^\ell - 1}{p - 1}\right) \\ (6.4) \quad &= (2^{k+1} - 1) \prod_{\substack{p^\ell \parallel m \\ p > 2}} \frac{p^{\ell+1} - 2}{p - 2} = mJ(m) \end{aligned}$$

by comparison with (3.5).

**Proposition 6.1.** *Let  $0 < \varepsilon \leq \frac{1}{2}$  be given. Suppose there exists a positive integer  $n(\varepsilon)$  such that*

$$(6.5) \quad (1 - \varepsilon) 2C_2 f(n) \frac{n}{\log^2 n} \leq R(2n) \leq (1 + \varepsilon) 2C_2 f(n) \frac{n}{\log^2 n}$$

for all  $n > n(\varepsilon)$ . Then there exists a constant  $m(\varepsilon)$  such that

$$(6.6) \quad (1 - 2\varepsilon)2C_2J(m)\frac{m}{\log^2 m} \leq a(2m) \leq (1 + 11\varepsilon)2C_2J(m)\frac{m}{\log^2 m}$$

for all  $m > m(\varepsilon)$ .

It is clear that Theorem 3.4 follows from Proposition 6.1, since Conjecture 3.3 implies that the hypothesis of Proposition 6.1 holds for every  $\varepsilon > 0$ .

*Proof of Proposition 6.1.* We shall not keep track explicitly of the necessary value for  $m(\varepsilon)$ , instead simply saying “when  $m$  is large enough” (in terms of  $\varepsilon$ ) in the appropriate places. We begin by writing

$$(6.7) \quad a(2m) = \sum_{c|2m} R(c) = \sum_{d|m} R(2d) = \sum_{\substack{d|m \\ d \leq m^{1-\varepsilon}}} R(2d) + \sum_{\substack{d|m \\ d > m^{1-\varepsilon}}} R(2d)$$

(where the second equality uses the fact that  $R(c) = 0$  when  $c$  is odd).

First we establish the upper bound in equation (6.6). We have  $m^{1-\varepsilon} > n(\varepsilon)$  when  $m$  is large enough, and so the summands in the second sum on the right-hand side of equation (6.7) can be bounded above by the upper bound in equation (6.5). For the first sum on the right-hand side we simply use the trivial bound  $R(2n) \leq n$ . The result is

$$\begin{aligned} a(2m) &\leq \sum_{\substack{d|m \\ d \leq m^{1-\varepsilon}}} d + \sum_{\substack{d|m \\ d > m^{1-\varepsilon}}} (1 + \varepsilon)2C_2f(d)\frac{d}{\log^2 d} \\ &\leq \sum_{\substack{d|m \\ d \leq m^{1-\varepsilon}}} m^{1-\varepsilon} + (1 + \varepsilon)2C_2\frac{1}{(1 - \varepsilon)^2 \log^2 m} \sum_{\substack{d|m \\ d > m^{1-\varepsilon}}} df(d) \\ &= m^{1-\varepsilon}\tau(m) + \frac{1 + \varepsilon}{(1 - \varepsilon)^2} \frac{2C_2}{\log^2 m} mJ(m) \end{aligned}$$

using the identity (6.4), where  $\tau(n)$  denotes the number of divisors of  $n$ . It is well known that  $\tau(m) \ll_\varepsilon m^{\varepsilon/3}$ , and so the first term is less than  $\varepsilon m / \log^2 m$  when  $m$  is large enough. Also  $(1 + \varepsilon)/(1 - \varepsilon)^2 \leq 1 + 10\varepsilon$  for  $0 < \varepsilon \leq \frac{1}{2}$ . Therefore

$$a(2m) \leq \varepsilon \frac{m}{\log^2 m} + (1 + 10\varepsilon) \frac{2C_2}{\log^2 m} mJ(m) \leq (1 + 11\varepsilon)2C_2J(m)\frac{m}{\log^2 m}$$

when  $m$  is large enough, since  $J(m) \geq 1$  for all positive integers  $m$  and  $2C_2 > 1$ . This establishes the upper bound in equation (6.6).

A similar method addresses the lower bound in equation (6.6). Since  $m^{1-\varepsilon} > n(\varepsilon)$  when  $m$  is large enough, the summands in the second sum on the right-hand side of equation (6.7) can be bounded below by the lower bound in equation (6.5); the first sum on the right-hand side is nonnegative, and so we can simply delete it.

We obtain the lower bound

$$\begin{aligned}
 a(2m) &\geq \sum_{\substack{d|m \\ d > m^{1-\varepsilon}}} (1+\varepsilon) 2C_2 f(d) \frac{d}{\log^2 d} \\
 (6.8) \quad &\geq (1-\varepsilon) \frac{2C_2}{\log^2 m} \sum_{\substack{d|m \\ d > m^{1-\varepsilon}}} df(d) = (1-\varepsilon) \frac{2C_2}{\log^2 m} \left( mJ(m) - \sum_{\substack{d|m \\ d \leq m^{1-\varepsilon}}} df(d) \right),
 \end{aligned}$$

again using the identity (6.4). This last sum is bounded above by

$$\sum_{\substack{d|m \\ d \leq m^{1-\varepsilon}}} df(d) \leq \sum_{d|m} \left( \frac{m^{1-\varepsilon}}{d} \right)^{1+\varepsilon/2} df(d) \leq m^{1-\varepsilon/2} \sum_{d|m} \prod_{\substack{p|d \\ p > 2}} \frac{p-1}{p^{\varepsilon/2}(p-2)}.$$

There are only finitely many primes  $p$  for which  $(p-1)/p^{\varepsilon/2}(p-2)$  exceeds 1, and so the inner product on the right-hand side is uniformly bounded by some constant  $C(\varepsilon)$ . Therefore

$$\sum_{\substack{d|m \\ d \leq m^{1-\varepsilon}}} df(d) \leq C(\varepsilon) m^{1-\varepsilon/2} \sum_{d|m} 1 = C(\varepsilon) m^{1-\varepsilon/2} \tau(m),$$

which as above is less than  $\varepsilon m$  for  $m$  large enough. Therefore equation (6.8) becomes

$$a(m) \geq (1-\varepsilon) \frac{2C_2}{\log^2 m} (mJ(m) - \varepsilon m) \geq (1-2\varepsilon) 2C_2 J(m) \frac{m}{\log^2 m}$$

when  $m$  is large enough, again since  $J(m) \geq 1$  always. This establishes the lower bound in equation (6.6).  $\square$

Before we begin the proof of Theorem 3.5, we will require a lemma regarding the function

$$Q(x) = \sum_{p+q \leq x} 1,$$

where  $p$  and  $q$  denote primes.

**Lemma 6.2.** *Uniformly for  $x \geq 3$ ,*

$$Q(x) = \frac{x^2}{2 \log^2 x} + O\left(\frac{x^2 \log \log x}{\log^3 x}\right).$$

*Proof.* We begin by writing

$$Q(x) = \sum_{p \leq x} \pi(x-p) = \sum_{x/\log x \leq p \leq x-\sqrt{x}} \pi(x-p) + O\left( \sum_{p \leq x/\log x} \pi(x-p) + \sum_{x-\sqrt{x} \leq p \leq x} \pi(x-p) \right).$$

Trivially  $\pi(x-p) \leq \pi(x) \leq x$ , so

$$\begin{aligned}
 Q(x) &= \sum_{x/\log x \leq p \leq x-\sqrt{x}} \pi(x-p) + O\left(\sum_{p \leq x/\log x} \pi(x) + \sum_{x-\sqrt{x} \leq p \leq x} x\right) \\
 &= \sum_{x/\log x \leq p \leq x-\sqrt{x}} \pi(x-p) + O\left(\pi(x)\pi\left(\frac{x}{\log x}\right) + x\sqrt{x}\right) \\
 (6.9) \quad &= \sum_{x/\log x \leq p \leq x-\sqrt{x}} \pi(x-p) + O\left(\frac{x^2}{\log^3 x}\right).
 \end{aligned}$$

In the main term, the prime number theorem gives

$$\sum_{x/\log x \leq p \leq x-\sqrt{x}} \pi(x-p) = \sum_{x/\log x \leq p \leq x-\sqrt{x}} \left( \text{li}(x-p) + O\left(\frac{x-p}{\log^2(x-p)}\right) \right)$$

(we could insert a better error term, but it would not improve the final result). Since  $x-p \geq \sqrt{x}$ , we have  $\log(x-p) \gg \log x$  and so

$$\begin{aligned}
 &= \sum_{x/\log x \leq p \leq x-\sqrt{x}} \text{li}(x-p) + O\left(\sum_{x/\log x \leq p \leq x-\sqrt{x}} \frac{x}{\log^2 x}\right) \\
 &= \sum_{x/\log x \leq p \leq x-\sqrt{x}} \text{li}(x-p) + O\left(\frac{x}{\log^2 x} \pi(x)\right) \\
 &= \sum_{x/\log x \leq p \leq x-\sqrt{x}} \text{li}(x-p) + O\left(\frac{x^2}{\log^3 x}\right),
 \end{aligned}$$

which transforms equation (6.9) into

$$(6.10) \quad Q(x) = \sum_{x/\log x \leq p \leq x-\sqrt{x}} \text{li}(x-p) + O\left(\frac{x^2}{\log^3 x}\right).$$

Using partial summation, we have

$$\begin{aligned}
 \sum_{x/\log x \leq p \leq x-\sqrt{x}} \text{li}(x-p) &= \int_{x/\log x}^{x-\sqrt{x}} \text{li}(x-t) d\pi(t) \\
 &= \pi(x-\sqrt{x}) \text{li}(\sqrt{x}) - \pi\left(\frac{x}{\log x}\right) \text{li}\left(x - \frac{x}{\log x}\right) + \int_{x/\log x}^{x-\sqrt{x}} \frac{\pi(t)}{\log(x-t)} dt,
 \end{aligned}$$

since the  $t$ -derivative of  $\text{li}(x-t)$  is  $-1/\log(x-t)$ . In other words,

$$\begin{aligned}
 \sum_{x/\log x \leq p \leq x-\sqrt{x}} \text{li}(x-p) &= O\left(x\sqrt{x} + \pi\left(\frac{x}{\log x}\right) \text{li}(x)\right) + \int_{x/\log x}^{x-\sqrt{x}} \frac{\pi(t)}{\log(x-t)} dt \\
 &= \int_{x/\log x}^{x-\sqrt{x}} \frac{\pi(t)}{\log(x-t)} dt + O\left(\frac{x^2}{\log^3 x}\right),
 \end{aligned}$$

and so equation (6.10) becomes

$$Q(x) = \int_{x/\log x}^{x-\sqrt{x}} \frac{\pi(t)}{\log(x-t)} dt + O\left(\frac{x^2}{\log^3 x}\right).$$



Using the prime number theorem again, this becomes

$$\begin{aligned}
 Q(x) &= \int_{x/\log x}^{x-\sqrt{x}} \frac{1}{\log(x-t)} \left( \frac{t}{\log t} + O\left(\frac{t}{\log^2 t}\right) \right) dt + O\left(\frac{x^2}{\log^3 x}\right) \\
 (6.11) \quad &= \int_{x/\log x}^{x-\sqrt{x}} \frac{t}{(\log t) \log(x-t)} dt + O\left( \int_{x/\log x}^{x-\sqrt{x}} \frac{t}{(\log^2 t) \log(x-t)} dt + \frac{x^2}{\log^3 x} \right).
 \end{aligned}$$

In the error term, again  $\log(x-t) \gg \log x$  and  $\log^2 t \gg \log^2 x$  due to the endpoints of integration, and so the entire integral is  $\ll x^2/\log^3 x$ . In the main term, we have

$$\log x \geq \log t \geq \log \frac{x}{\log x} = \log x - \log \log x = (\log x) \left( 1 + O\left(\frac{\log \log x}{\log x}\right) \right),$$

and therefore equation (6.11) becomes

$$(6.12) \quad Q(x) = \frac{1}{\log x} \left( 1 + O\left(\frac{\log \log x}{\log x}\right) \right) \int_{x/\log x}^{x-\sqrt{x}} \frac{t}{\log(x-t)} dt + O\left(\frac{x^2}{\log^3 x}\right).$$

Finally,

$$\begin{aligned}
 \int_{x/\log x}^{x-\sqrt{x}} \frac{t}{\log(x-t)} dt &= \int_0^{x-2} \frac{t}{\log(x-t)} dt + O\left( \int_0^{x/\log x} t dt + \int_{x-\sqrt{x}}^{x-2} t dt \right) \\
 &= \int_2^x \frac{x-u}{\log u} du + O\left(\frac{x^2}{\log^2 x}\right) \\
 (6.13) \quad &= x \operatorname{li}(x) - \int_2^x \frac{u}{\log u} du + O\left(\frac{x^2}{\log^2 x}\right).
 \end{aligned}$$

By integration by parts, this integral is

$$\begin{aligned}
 \int_2^x \frac{u}{\log u} du &= \frac{u^2}{2} \frac{1}{\log u} \Big|_2^x + \int_2^x \frac{u^2}{2} \frac{1}{u \log^2 u} du \\
 &= \frac{x^2}{2 \log x} + O\left( 1 + \int_2^{\sqrt{x}} \frac{u}{\log^2 u} du + \int_{\sqrt{x}}^x \frac{u}{\log^2 u} du \right) \\
 &= \frac{x^2}{2 \log x} + O\left( \sqrt{x} \cdot x + x \frac{x}{\log^2 x} \right) = \frac{x^2}{2 \log x} + O\left(\frac{x^2}{\log^2 x}\right).
 \end{aligned}$$

Therefore equation (6.13) becomes

$$\int_{x/\log x}^{x-\sqrt{x}} \frac{t}{\log(x-t)} dt = x \operatorname{li}(x) - \frac{x^2}{2 \log x} + O\left(\frac{x^2}{\log^2 x}\right) = \frac{x^2}{2 \log x} + O\left(\frac{x^2}{\log^2 x}\right)$$

by the fact that  $\operatorname{li}(x) = x/\log x + O(x/\log^2 x)$ . Using this in equation (6.12) finally yields

$$\begin{aligned}
 Q(x) &= \frac{1}{\log x} \left( 1 + O\left(\frac{\log \log x}{\log x}\right) \right) \left( \frac{x^2}{2 \log x} + O\left(\frac{x^2}{\log^2 x}\right) \right) + O\left(\frac{x^2}{\log^3 x}\right) \\
 &= \frac{x^2}{2 \log^2 x} + O\left(\frac{x^2 \log \log x}{\log^3 x}\right),
 \end{aligned}$$

as claimed.  $\square$

Equipped with Lemma 6.2, we are now prepared to prove Theorem 3.5.

*Proof of Theorem 3.5.* Starting with the definitions of  $a(m)$  and  $A(M)$ , we have

$$A(M) = \sum_{m=1}^{2M} a(m) = \sum_{m=1}^{2M} \sum_{d|m} R(d) = \sum_{m=1}^{2M} \sum_{d|m} \sum_{p+q=d} 1 = \sum_{p+q \leq 2M} \sum_{\substack{1 \leq m \leq 2M \\ (p+q)|m}} 1.$$

Writing  $m = (p+q)n$ , we obtain  
(6.14)

$$A(M) = \sum_{p+q \leq 2M} \sum_{1 \leq n \leq 2M/(p+q)} 1 = \sum_{1 \leq n \leq M/2} \sum_{p+q \leq 2M/n} 1 = \sum_{1 \leq n \leq M/2} Q\left(\frac{2M}{p+q}\right).$$

The trivial bound  $Q(x) \leq x^2$  allows us to write

$$A(M) = \sum_{1 \leq n \leq \log^3 M} Q\left(\frac{2M}{n}\right) + O\left(\sum_{n > \log^3 M} \left(\frac{2M}{n}\right)^2\right) = \sum_{1 \leq n \leq \log^3 M} Q\left(\frac{2M}{n}\right) + O\left(\frac{M^2}{\log^3 M}\right),$$

since  $\sum_{n > \log^3 M} n^{-2} \ll 1/\log^3 M$  by comparison with an integral. We use Lemma 6.2 to get

$$\begin{aligned} A(M) &= \sum_{1 \leq n \leq \log^3 M} \left( \frac{(2M/n)^2}{2 \log^2(2M/n)} + O\left(\frac{(2M/n)^2 \log \log(2M/n)}{\log^3(2M/n)}\right) \right) + O\left(\frac{M^2}{\log^3 M}\right) \\ &= 2M^2 \sum_{1 \leq n \leq \log^3 M} \frac{1}{\log^2(2M/n)} \frac{1}{n^2} + O\left(\sum_{1 \leq n \leq \log^3 M} \frac{\sqrt{2M} \log \log 2M}{\log^3 2M} \left(\frac{2M}{n}\right)^{3/2} + \frac{M^2}{\log^3 M}\right), \end{aligned}$$

since  $\sqrt{x} \log \log x / \log^3 x$  is an (eventually) increasing function of  $x$ . By the convergence of  $\sum_n n^{-3/2}$ , we obtain

$$A(M) = 2M^2 \sum_{1 \leq n \leq \log^3 M} \frac{1}{\log^2(2M/n)} \frac{1}{n^2} + O\left(\frac{M^2 \log \log M}{\log^3 M}\right).$$

Finally, we have  $\log(2M/n) = \log M - \log(n/2) = \log M + O(\log(\log^3 M)) = (\log M)(1 + O(\log \log M / \log M))$  as before. Therefore

$$A(M) = \frac{2M^2}{\log^2 M} \left(1 + O\left(\frac{\log \log M}{\log M}\right)\right) \sum_{1 \leq n \leq \log^3 M} \frac{1}{n^2} + O\left(\frac{M^2 \log \log M}{\log^3 M}\right).$$

We conclude that

$$\begin{aligned} A(M) &= \frac{2M^2}{\log^2 M} \left(1 + O\left(\frac{\log \log M}{\log M}\right)\right) \left(\zeta(2) + O\left(\frac{1}{\log^3 M}\right)\right) + O\left(\frac{M^2 \log \log M}{\log^3 M}\right) \\ &= \frac{\pi^2 M^2}{3 \log^2 M} + O\left(\frac{M^2 \log \log M}{\log^3 M}\right), \end{aligned}$$

as desired.  $\square$

## REFERENCES

- [1] P.T. Bateman and H.G. Diamond, *Analytic number theory*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2004, An introductory course.
- [2] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979
- [3] G.H. Hardy and J.E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70.

- [4] M.N. Huxley, *Exponential sums and lattice points III*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 591–609
- [5] H. Li, *The exceptional set of Goldbach numbers. II*, Acta Arith. **92** (2000), no. 1, 71–88.
- [6] H.L. Montgomery and R.C. Vaughan, *The exceptional set in Goldbach's problem*, Collection of articles in memory of Juriĭ Vladimirovič Linnik, Acta Arith., **27** (1975), 353–370.

SIMON FRASER UNIVERSITY, DEPARTMENT OF MATHEMATICS, 8888 UNIVERSITY DRIVE, BURNABY, BC V5A 1S6, CANADA

UNIVERSITY OF BRITISH COLUMBIA, DEPARTMENT OF MATHEMATICS, 1984 MATHEMATICS ROAD, VANCOUVER, BC V6T 1Z2, CANADA